УТВЕРЖДЕН

643.53262993.00021–01 92– ЛУ

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ
«ПАНЦИРЬ+» ДЛЯ ОС MICROSOFT WINDOWS

Назначение и задачи, решаемые механизмами защиты

643.53262993.00021–01 92

Листов 14

Подп. и дата	
Инв.№ дубл.	
Взам.инв.№	
Подп. и дата	
Инв.№ подл	

Санкт–Петербург

2016

Аннотация

В данном документе рассматриваются назначение и задачи, решаемые механизмами защиты Комплексной системой защиты информации «Панцирь+» для ОС Microsoft Windows (далее КСЗИ «Панцирь+»), обозначение 643.53262993.00021–01, Сертификат соответствия ФСТЭК России № 3473 от 17.12.2015. КСЗИ «Панцирь+» является инновационным средством защиты, как в части решаемых им задач защиты, так и в части реализованных технологий защиты и технических решений, в том числе запатентованных, что принципиально отличает КСЗИ «Панцирь+» от иных средств защиты информации. В данном документе кратко изложены данные отличия. В документе приводится систематизированный взгляд на подходы к реализации защиты информации КСЗИ «Панцирь+» и к использованию включенных в ее состав механизмов защиты.

Оглавление

1. Назначение

Согласно документу ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения» КСЗИ «Панцирь+» является средством защиты информации от несанкционированного доступа, поскольку его применение направлено на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации – с нарушением разграничительной политики доступа. Основу КСЗИ «Панцирь+» составляют механизмы контроля и разграничения прав доступа к ресурсам информационной системы.

Построение разграничительной политики доступа в КСЗИ «Панцирь+» предполагает решение следующих взаимосвязанных задач защиты:

- формирование и разделение режимов обработки информации в информационной системе – реализованы ролевая и сессионная модели контроля доступа;
- обеспечение корректности (защиты от обхода) разграничительной политики доступа;
- защита системных объектов;
- защита от вторжений в информационную систему.

2. Формирование и разделение режимов обработки информации

2.1. Ролевая модель контроля доступа

Методы дискреционного контроля доступа в известных СЗИ НСД направлены на реализацию защиты критичных объектов, в том числе файловых, от несанкционированного к ним доступа. При этом назначаются права (правила) доступа к объектам субъектов – пользователей, и именно объект, как элемент защиты, является ключевым компонентом в реализации разграничительной политики доступа.

В КСЗИ «Панцирь+» методом дискреционного контроля доступа к статичным объектам реализуется ролевая модель контроля доступа. В общем случае ролевая модель контроля доступа (Role–Based Access Control – RBAC) предназначена не для защиты конкретных объектов от несанкционированного к ним доступа, а для формирования и при необходимости разделения режимов обработки информации пользователями в рамках выполняемых ими ролей в информационной системе. Целью использования ролевой модели контроля доступа является предоставление пользователю права доступа только к необходимым для исполнения роли объектам необходимыми средствами (программы или процессы), включая обработку только необходимой информации для реализации роли. При этом в КСЗИ «Панцирь+» назначаются права (правила) доступа субъектов к объектам (а не наоборот, как в известных решениях), поскольку именно субъектом (ролью) определяется критичность обрабатываемой информации в рамках реализации роли, и, как следствие, именно субъект (роль) является ключевым компонентом в реализации разграничительной политики доступа. Разделение режимов информации требуется в том случае, когда не допустимым является перенос информации, обрабатываемой в одной роли, в другую роль, характеризуемую иным режимом (иными условиями) ее обработки, в частности требованиями к защите.

Роль в КСЗИ «Панцирь+» идентифицируется учетной записью, для этого для работы пользователя в конкретной роли создается своя учетная запись. В случае, если доступ к роли между различными пользователями (физическими лицами) не разграничивается (разграничивается доступ к ресурсам исключительно между ролями), то различные пользователи в одной роли могут работать под одной и той же учетной записью. В КСЗИ «Панцирь+» выбор роли пользователем при входе в систему осуществляется регистрацией под соответствующей учетной записью, смена роли – штатными средствами смены учетной записи.

Это единственно корректная, по мнению разработчиков КСЗИ «Панцирь+», реализация ролевой модели контроля доступа, требующей разделения режимов обработки

информации, создаваемых для различных ролей. Это объясняется тем, что реализация сущности «роль» в качестве субъекта доступа, для которой могла бы строиться разграничительная политика доступа, т.е. реализация возможности работы пользователя под одной учетной записью в различных ролях, является потенциально опасным решением, поскольку при необходимости выполнения требования к разграничению прав доступа к информации, обрабатываемой в различных ролях (она может обладать различным уровнем критичности к хищению, либо к несанкционированной модификации) − к разделению режимов обработки информации, создаются дополнительные каналы несанкционированного обмена информацией между ролями. Вызвано это тем, что основу разграничительной политики доступа в современных ОС Windows составляет реализация разграничений, в том числе, ко многим объектам «по умолчанию» (без вынесения соответствующих настроек в интерфейс), именно между учетными записями, которые будут отсутствовать между ролями, при условии реализации возможности работы пользователя в различных ролях под одной и той же учетной записью.

Использование сервера безопасности КСЗИ «Панцирь+» значительно упрощает задачу создания ролей (учетных записей, идентифицирующих роль) в доменной архитектуре. Сервер безопасности КСЗИ «Панцирь+» отвечает за создание доменных учетных записей и их распространение на клиентские части КСЗИ «Панцирь+».

Возможности ролевой модели контроля доступа в КСЗИ «Панцирь+» принципиально расширены включением в субъект доступа сущности «процесс» – субъект доступа определяется парой сущностей: учетная запись (идентификатор роли) и процесс, объединяемых в разграничительной политике доступа в единую сущность «профиль». В КСЗИ «Панцирь+» права доступа к ресурсам назначаются для профилей. Это позволяет разграничивать не только то, к какому ресурсу и какие права доступа имеет пользователь в рамках выполнения роли, но и то, каким процессом (приложением), т.е., какими средствами, пользователь может осуществить доступ к ресурсу в рамках выполнения роли. Существенное упрощение настройки разграничений прав доступа для создаваемых подобным образом ролей, в том числе, с учетом их иерархии, достигается возможностью создания нового профиля (разграничительной политики доступа для профиля) на основе существующих профилей, по средством модификации заданных для них правил доступа.

Важнейшим механизмом защиты из состава КСЗИ «Панцирь+» при реализации ролевой модели контроля доступа является механизм управления монтированием устройств по пользователям (соответственно, по ролям). Для каждой роли этим механизмом защиты можно сформировать – локализовать, свой набор устройств, включая

системные и подключаемые в процессе работы, в том числе, файловые накопители, идентифицируемые их серийными номерами, прошитыми в устройствах изготовителями этих устройств. Важность управления монтированием/отмонтированием (в том числе динамическим) системных устройств обусловливается потенциальной опасностью подобных устройств (встроенный микрофон, камера, сетевые адаптеры и т.д.) для их несанкционированного использования.

В результате локализации разрешенного набора устройств для роли определяются ресурсы, к которым требуется разграничивать права доступа.

Другой соответствующей задачей локализации является задача локализации субъектов доступа «процесс» − обеспечение замкнутости программной среды, позволяющий для любой роли и для компьютера в целом задать разрешенный для использования набор процессов (приложений). Данная задача в КСЗИ «Панцирь+» решается механизмом дискреционного управления доступом к исполняемым файлам и может усиливаться заданием соответствующей политики доступа к типам файлов, а также запретом на исполнение создаваемых в системе файлов механизмом дискреционного управления доступом к создаваемым файлам.

КСЗИ «Панцирь+» предоставляет все необходимые возможности в части реализации контроля доступа ролей (профилей, идентифицирующих роль) к ресурсам, позволяя осуществить контроль доступа ко всем значимым ресурсам:

- к **файловым объектам**. Контроль доступа к файловым объектам значительно расширен возможностью разграничения прав доступа к типам файлов, что позволяет работать определенным приложениям только с определенными типами файлов, сохранять на внешних накопителях, передавать по сети и т.д. Контроль доступа к файловым объектам применим и к локальным, и к разделенным в сети ресурсам;
- к **файловым накопителям** и к к**онкретным файловым объектам на файловых накопителях**. Файловый накопитель идентифицируется в разграничительной политике доступа не буквой диска, а своим идентификатором, включая серийный номер устройства, прошитый в устройстве изготовителем данного устройства;
- к **локальным** и **разделенным в сети принтерам**;
- к **сетевым объектам**. Контроль доступа к сетевым объектам реализован локальным сетевым экраном, позволяющим не только разграничивать права доступа профилей к отдельным объектам, но и фильтровать заголовки пакетов (исходящих и входящих) по всем значимым полям. При этом для каждого сетевого адаптера могут назначаться свои правила доступа – какие учетные записи, какими приложениями, к

каким объектам (адреса и номера портов), с использованием каких протоколов и каких сетевых служб и т.д. могут осуществлять доступ к сетевым объектам.

Ресурсы, характеризуемые только одним правом доступа – использовать или нет, например, сканеры, могут контролироваться механизмом управления монтированием устройств по пользователям (по ролям, для механизма управления монтированием устройств роль определяется учетной записью пользователя).

Важнейшим универсальным механизмом защиты из состава КСЗИ «Панцирь+», обеспечивающим возможность создания регламентов работы с приложениями (по дням недели, времени, продолжительности и т.д.) является механизм управления процессами, позволяющий для любого приложения задать временные параметры работы с приложением, что крайне важно при реализации ролевой модели контроля доступа. При задании соответствующих временных режимов работы для системного процесса winlogon реализуется временной регламент работы защищаемого компьютера.

2.2. Сессионная модель контроля доступа

Сессионная модель контроля доступа также предполагает создание, но в данном случае уже обязательное разделение, режимов обработки информации различных категорий конфиденциальности, в данном случае обработка информации определяется уровнем конфиденциальности – сессией. Т.е. для данной модели контроля доступа режим – сессия, определяется не ролью пользователя в информационной системе, а уровнем конфиденциальности обрабатываемой им информации.

В общем случае на одном и том же компьютере одним и тем же пользователем, естественно, в различных режимах, характеризуемых различными требованиями к защите, должна обрабатываться информация различных уровней конфиденциальности, при условии предотвращения перемещения информации более высокого уровня конфиденциальности в менее защищенный режим обработки информации более низкого уровня конфиденциальности.

Как следствие, по мнению разработчиков КСЗИ «Панцирь+», в данном случае включение в разграничительную политику доступа некой сущности «сессия», с учетом всего сказанного ранее, является не просто опасным (как включение сущности «роль»), а недопустимым решением. Безопасным решением является создание (по аналогии с ролевой моделью) пользователю для работы в каждой сессии своей учетной записи. Выбор сессии пользователем при входе в систему при этом осуществляется регистрацией под соответствующей учетной записью, смена сессии – штатными средствами смены учетной записи.

Основу реализации сессионной модели контроля доступа в КСЗИ «Панцирь+» составляет использование метода мандатного контроля доступа к создаваемым файлам. Данный метод контроля доступа характеризуется предельной простотой администрирования – требуется назначать метки безопасности (мандаты или уровни доступа) исключительно учетным записям (сессиям) – не требуется назначения каких–либо меток объектам доступа, а также корректностью реализации разграничительной политики доступа, в том числе, и в части контроля доступа к неразделяемым системой и приложениями файловым объектам.

С учетом того, что в КСЗИ «Панцирь+» сессия идентифицируется учетной записью, в рамках реализации сессионной модели контроля доступа с целью реализации режимов обработки информации – сессий, могут быть использованы возможности управления монтирования устройств и все возможности контроля доступа, что и при реализации ролевой модели контроля доступа, описанные выше. С учетом же того, что ресурсы в общем случае не подпадают под иерархические признаки конфиденциальности обрабатываемой информации – ресурс может использоваться для работы с информацией не ниже определенного уровня, не выше определенного уровня, с конкретным уровнем конфиденциальности информации, разграничительная политика доступа в КСЗИ «Панцирь+» для сессии к ресурсам не являющимся файловыми объектами реализуется перечислением сессий (учетных записей), которыми может использоваться соответствующий ресурс (например, устройство), что предусмотрено в интерфейсах соответствующих механизмов защиты.

Возможности сессионной, как и ролевой, модели контроля доступа в КСЗИ «Панцирь+» значительно расширены возможностью дополнительно реализовать в рамках каждой сессии разграничивать права доступа к ресурсам для приложений. Одновременно может быть реализована и ролевая, и мандатная схема контроля доступа, при этом доступ к ресурсу становится возможным в случае его непротиворечивости и мандатным, и дискреционным правилам контроля доступа.

Метод дискреционного контроля доступа может использоваться и для реализации разграничительной политики доступа между различными пользователями при их работе в одной сессии.

3. Обеспечение корректности (защиты от обхода) разграничительной политики доступа

Обеспечение корректности разграничительной политики доступа требует решения множества вспомогательных задач защиты, направленных на реализацию защиты от обхода заданных правил доступа к ресурсам с целью получения несанкционированного доступа к обрабатываемой информации. Без решения этих ключевых задач о какой–либо эффективности защиты говорить не приходится.

В КСЗИ «Панцирь+» к таким важнейшим механизмам защиты могу быть отнесены:

1. Механизм управления монтированием устройств, позволяющий предотвратить монтирование к системе устройств, предназначенных для хранения информации, но не являющихся файловыми накопителями – к ним не разграничиваются права доступа, как к файловым объектам (например, к таким устройствам относится ряд смартфонов).

2. Механизм перенаправления запросов доступа, позволяющий для любого процесса, в том числе системного, разделить не разделяемые файловые объекты (файлы и каталоги), за счет переадресации запросов доступа в копии неразделяемых объектов, создаваемые для различных субъектов, без чего невозможна в общем случае реализация разделения режимов обработки информации.

3. Механизм управления прямым доступом к дискам (к жесткому диску и к отчуждаемым накопителям). Такой возможностью обладают не только некоторые специальные утилиты, но и ряд текстовых редакторов при использовании ими соответствующих плагинов. В общем случае потенциально любое приложение при определенных условиях может обладать подобной возможностью. Для каждого процесса в КСЗИ «Панцирь+» можно контролировать и при необходимости предотвращать прямой доступ к дискам, который реализуется в обход разграничений прав доступа к файловым объектам.

4. Механизм управления олицетворением. В современных ОС Windows для процесса существует возможно осуществить запрос и получить от системы права другого пользователя, с которыми далее в обход разграничительной политики доступа осуществить несанкционированный доступ к объектам. Это крайне опасная возможность, связанная с повышением привилегий. Для каждого процесса в КСЗИ «Панцирь+» можно контролировать и при необходимости предотвращать использование сервисов олицетворения с целью получения прав иного пользователя.

5. Механизм гарантированного удаления файловых объектов. При удалении файла системными средствами собственно данные не удаляются – удаляется разметка соответствующего файла. В результате этого данные из удаленных файлов образуют, так называемую остаточную информацию, к которой можно осуществить доступ. В КСЗИ «Панцирь+» реализована возможность гарантированного удаления (удаление остаточной информации) файловых объектов как на жестком диске, так и на внешних накопителях, что можно настроить для любых папок, используемых для хранения обрабатываемой информации (к статичным объектам), либо для любых субъектов доступа – все создаваемые ими файлы при удалении будут гарантированно удаляться.

6. Механизм очистки ОЗУ. При старте процесса системой для него выделается соответствующая область оперативной памяти. При завершении процесса, она не очищается, что потенциально позволяет получить несанкционированный доступ к данной остаточной информации. В КСЗИ «Панцирь+» осуществляется принудительная очистка освобождаемых областей оперативной памяти при следующих условиях: при регистрации нового пользователя, завершении работы пользователя, либо при запуске нового процесса, завершении процесса.

4. Защита системных объектов

К системным объектам могут быть отнесены соответствующие системные файловые объекты – исполняемые файлы и конфигурационные файлы системы и приложений, а также объекты реестра ОС.

В КСЗИ «Панцирь+» к данным объектам реализуется разграничительная политика доступа, причем, как для пользователей, так, что принципиально важно, для процессов. При этом для субъектов доступа можно разрешить доступ только к необходимым системным объектам доступа для корректного функционирования, что реализуется следующими механизмами защиты:

- механизмом управления доступом к статичным файловым объектам (в данном случае, к системным файловым объектам);
- механизмом управления доступом к объектам реестра ОС.

5. Защита от вторжений. Процессная модель контроля доступа

Вторжение в информационную систему реализуется процессом с использованием той или иной уязвимости, с целью получения несанкционированного доступа к информации, обрабатываемой иными процессами, либо с целью запуска вредоносной программы, которая может реализовывать различные варианты обхода разграничительной политики доступа.

Источниками реализации атаки со стороны санкционированных процессов являются возможность наделения их вредоносными свойствами, как с использованием их штатных возможностей, например, в результате чтения вредоносного командного файла – скрипта и т.д., так и в результате использования выявленной ошибки программирования в исполняемом файле процесса, что может быть осуществлено, как в отношении процессов приложений, так и в отношении системных процессов. Получение доступа процессом к информации, обрабатываемой иными процессами, обусловливается невозможностью задания в системе различных разграничений для различных процессов – любой запускаемый в системе процесс наследует права доступа к ресурсам запустившего его пользователя.

Процессная модель контроля доступа предназначена для формирования и при необходимости разделения режимов обработки информации процессами в рамках решаемых ими задач обработки информации. Таким образом, реализация процессной модели состоит в реализации разграничительной политики доступа для процессов к ресурсам.

В части контроля доступа ко всем статичным (присутствующим в системе на момент задания разграничительной политики доступа) ресурсам в КСЗИ «Панцирь+» реализована процессная модель контроля доступа, поскольку права доступа процессов могут быть разграничены к файловым объектам, к объектам реестра ОС, к сетевым объектам и т.д., что описано ранее.

Задача защиты от наделения процесса вредоносными свойствами за счет прочтения ими вредоносных командных файлов в КСЗИ «Панцирь+» решается расширением механизма дискреционного управления доступом к статичным файловым объектам, за счет реализации контроля доступа к типам файлов. Решение задачи состоит в том, что процессам может запрещаться создание новых командных файлов, идентифицируемых по их расширениям, в том числе, и по средством переименования в подобные файлы (переименование расширений). В результате этого занесение нового командного файла на защищаемый компьютер предотвращается, а пользователь попутно освобождается от

ненужной ему баннерной рекламы при работе с сетью. Подобное же решение может быть реализовано и в отношении исполняемых файлов.

Для защиты от запуска вредоносных программ и для разделения режимов обработки информации различными процессами в КСЗИ «Панцирь+» реализованы механизмы управления доступом к создаваемым объектам:

- механизм управления доступом к создаваемым файлам;
- механизм управления доступом к буферу обмена.

Основаны данные механизмы защиты на автоматической разметке КСЗИ «Панцирь+» создаваемых файлов и данных, помещаемых в буфер обмена. Разметка – это учетные данные субъекта, создавшего объект – учетная запись, имя процесса (полнопутевое имя исполняемого файла), метка безопасности (при реализации метода мандатного управления доступом, используемого в сессионной модели контроля доступа). Это позволяет задавать разграничительную политику доступа следующим образом принципиально упрощающим задачу администрирования к создаваемым объектам:

- запрет запуска (исполнения), в том числе и системными пользователями, любого создаваемого в системе объекта – защита от запуска вредоносных программ;
- назначение прав доступа субъекта к объектам, созданным иными субъектами (объект доступа исключается из разграничительной политики доступа – назначаются не правила доступа субъектов к объектам, а правила доступа между субъектами к создаваемым ими объектам, по следующему принципу – одному субъекту доступа разрешаются/запрещаются какие–то права доступа к объектам, созданным другим субъектом доступа) – разделение режимов обработки информации процессами.

Поскольку вторжение в систему может быть реализовано процессом, а при реализации процессной модели контроля доступа действия процессов (по крайней мере, критичных в части возможности реализации на них атаки), по средством реализации соответствующей разграничительной политики доступа, локализуются, причем в части их прав доступа, как к статичным, так и к создаваемым объектам, то использование процессной модели контроля доступа может позиционироваться, как реализация защиты от вторжений в информационную систему. При этом крайне важно, что данное решение призвано не обнаруживать вторжения с использованием соответствующих журналов безопасности, а именно в реальном времени за счет реализации разграничительной политики доступа для процессов, реализовывать защиту от вторжений в реальном масштабе времени.

Поскольку данная функциональная задача защиты требует немедленного уведомления администратора безопасности о зарегистрированной попытке вторжения в

систему, в КСЗИ «Панцирь+» реализован режим аудита событий безопасности реального времени, предполагающий возможность задания для любого критичного контролируемого события в рамках реализации процессной модели контроля доступа, режима отправки соответствующего сообщения в реальном времени на отдельный компонент системы защиты – сервер аудита. Реализован в КСЗИ «Панцирь+» и инструментальный аудит событий безопасности, используемый для формирования режимов обработки информации процессами при настройке разграничения их прав доступа к статичным объектам. Используя инструментальный аудит, можно установить правила аудита доступа любого процесса к любому объекту и определить необходимые ему для корректного функционирования права доступа к этому объекту.

Реализованные в КСЗИ «Панцирь+» подходы к защите информации в общем случае отличает следующее:

- права доступа субъектов к объектам назначаются субъектам доступа, что позволяет, не только расширить функциональные возможности механизмов защиты, но и использовать при назначении правил доступа маски и переменные среды окружения. Это, в свою очередь, позволяет упростить настройку разграничительной политики доступа и, что немало важно, унифицировать настройки разграничительной политики доступа для различных защищаемых компьютеров;
- хранение правил доступа не в виде атрибутов доступа к объектам, а в виде отдельной матрицы доступа – в отдельных файлах, с учетом возможности унифицировать настройки разграничительной политики доступа для различных защищаемых компьютеров за счет использования масок и переменных среды окружения, позволяет решить задачу удаленного тиражирования настроек с сервера безопасности КСЗИ «Панцирь+», что принципиально упрощает задачу реализации процессной модели контроля доступа. Данная задача решается отдельной программой из состава КСЗИ «Панцирь+» – программой тиражирования настроек.

6. Список сокращений

СЗИ НСД	Средства защиты информации от несанкционированного доступа
ОС	Операционная система
ОЗУ	Оперативное запоминающее устройство